UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF NORTH CAROLINA

Detrina Solomon, on her own behalf and on behalf of those similarly situated, Plaintiff, v. ECL Group, LLC Defendant.	**Case No. 1:22-cv-00526** **COMPLAINT – CLASS ACTION** **Jury Trial Demanded**

Plaintiff Detrina Solomon ("Plaintiff"), by and through her attorneys of record, upon personal knowledge as to her own acts and experiences, and upon information and belief as to all other matters, files this complaint against ECL Group, LLC ("Eye Care Leaders" or "Defendant") and alleges the following:

INTRODUCTION

1. Plaintiff brings this class action complaint on behalf of a class of persons impacted by Defendant's failure to safeguard, monitor, maintain and protect highly sensitive Personal Health Information ("PHI") and Personally Identifiable Information ("PII") (collectively "Sensitive Information"). Eye Care Leaders is a vendor that provides patient management software to its client eye care clinics which, among other things, manages patients' electronic health records. As part of its services, Defendant collected, stored, and maintained Plaintiff's and the Class's Sensitive Information, which Plaintiff provided to Eye Care Leaders' client Eye Mart.

2. Starting around December 4, 2021, Defendant experienced a cyberattack during which criminal hackers obtained access to Plaintiff and the Class's Sensitive Information ("Data Breach"). During the Data Breach, criminal hackers infiltrated and obtained control over Defendant's systems, specifically, its myCare Identity solution, which is Eye Care Leaders' medical record platform. Access to this platform provided the hackers access to Plaintiff's and the Class's Sensitive Data. Criminal hackers were fully capable of viewing, copying, and exfiltrating patients' Sensitive Information.

3. Defendant's response has been sporadic and it still does not appear to have a complete understanding of the full scope of the Data Breach. As such, its notices to its clients have been piecemeal. While Eye Care Leaders provided notice to some impacted clinics in March 2022, others appear to have only recently received notice. In fact, some clinics issued notice to their patients as recently as June 2, 2022 that they were impacted by Eye Care Leaders's Data Breach, a delay of six months after the Data Breach.

4. Although Eye Care Leaders is the only entity that knows the full scope of its breach, it did not issue notice directly to impacted individuals, but rather, required its clients to notify their impacted patients. The clinics' notices of the Data Breach, however, appear to have been drafted by Eye Care Leaders, and all make clear that Eye Care Leaders, not the clinic, was breached. The notices state that Defendant experienced a cyberattack that exposed highly Sensitive Information, including: patient names, dates of birth, medical record numbers, health insurance information, Social Security numbers, and information regarding the care patients' received at each eye care practice.

5. Due to its direct access to Eye Care Leaders' medical records platform, hackers had the opportunity to obtain, sell, and misuse patients' Sensitive Information without their knowledge, leaving patients with no opportunity to take measures to protect themselves from the known, significant risk of harm that occurs when cybercriminals obtain Sensitive Information in a data breach. That harm includes the risk of health insurance fraud, medical fraud, credit card fraud, and identity theft, among others.

6. As a result of Defendant's lax data security, malicious cybercriminals have accessed the most sensitive details of the lives and the identities of hundreds of thousands of patients. Due to Eye Care Leaders' delayed notice of its Data Breach, the exact number of impacted individuals is unknown. However, from notices provided by Eye Care Leaders' clients, the Data Breach appears to have impacted at least 348,000 and likely many more. Because that number was determined from only a handful of clients, and Eye Care Leaders serves over 9,000 physicians, the number of individuals impacted is likely far higher.

7. Because the Data Breach compromised Plaintiff's Sensitive Information, Plaintiff and the Class (defined below) have been placed in an immediate and continuing risk of harm from fraud, identity theft, and related harm caused by the Data Breach.

8. As a result of Defendant's conduct, Plaintiff and the Class have and will be required to continue to undertake time-consuming and often costly efforts to mitigate the actual and potential harm caused by the Data Breach. This includes efforts to mitigate the breach's exposure of their Sensitive Information, including by, among other things, placing

freezes and setting alerts with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, reviewing and monitoring credit reports and accounts for unauthorized activity, changing passwords on potentially impacted websites and applications, and requesting and maintaining accurate medical records. Minors may not be able to monitor the impact of the Data Breach on their lives for years, at which point the damage will be done.

9. Plaintiff and the Class bring this action to recover for the harm they suffered, and assert the following claims: negligence, negligence *per se*, violation of the North Carolina Unfair and Deceptive Trade Practices Act, and declaratory judgment.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this case pursuant to 28 U.S.C. § 1332(d), the Class Action Fairness Act, which affords federal courts with original jurisdiction over cases where any member of the plaintiff class is a citizen of a state different from any defendant, and where the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Here, Plaintiff is diverse from Defendant because Defendant resides in the State of North Carolina, where they operate their principal headquarters, and the State of Washington, where it is incorporated. Plaintiff resides in the State of Texas.

11. This Court has general personal jurisdiction over Defendant because Defendant operates its principal place of business in this State. Additionally, this Court also has specific personal jurisdiction over Defendant because it has minimum contacts

with this State, as it is located and conducts substantial business here, and Plaintiff's claims arise from Defendant's conduct in this State.

12. This Court is the proper venue for this action pursuant to 28 U.S.C. § 1391(a) and (b) because a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in this District and because Defendant conducts a substantial part of its business within this District.

PARTIES

13. **Plaintiff** Detrina Solomon is a patient of an eyecare clinic in Texas that uses Eye Care Leaders as a vendor. Solomon received a notice that her information was impacted by Eye Care Leader's Data Breach. Subsequently, Solomon has noticed an increase in spam texts, spam calls, and spam emails. The high number of spam calls prompted Solomon to change her phone numbers. Additionally, she has changed passwords on her personal accounts to prevent any identity theft.

14. **Defendant** ECL Group, LLC is a North Carolina limited liability company with its principal place of business in Durham, North Carolina. Eye Care Leaders provides services to approximately 9,000 eye care doctors throughout the country and, specifically, provides software and technology to help clinics manage, among other things, patient medical records, scheduling and visit information, and billing.

FACTUAL BACKGROUND

A. Eye Care Leaders Collected, Maintained and Stored Sensitive Information

15. Eye Care Leaders claims to be the "No. 1 source for the top-rated ophthalmology-specific EHR [or Electronic Health Records] and Practice Management systems."[1] Specifically, Eye Care Leaders provides medical records platforms and patient management software to eye care clinics throughout the nation, including, purportedly, to more than 9,000 physicians.[2] It claims to offer the best eye care clinic technology solutions available anywhere in the market, including a "power family of new and existing solutions that can improve, enhance, and coordinate every level of eye care management."[3] These solutions are cloud-based, meaning the data, including patient information, is stored on Eye Care Leaders's servers and accessed by clinics and staff.

16. Through its services, Eye Care Leaders gains access to and control over Plaintiff's personal and medical information. Specifically, patients, like Plaintiff and the Class, must provide their physicians and clinics with highly sensitive information, including PHI, PII, or both, to obtain treatment. Clinics, in turn, enter that Sensitive Information into Defendant's software programs and electronic records platforms, whereupon Defendant compiles, stores, and maintains the highly sensitive PII and PHI concerning, among other things, patients' medical diagnostics, treatment, and other

[1] *About Eye Care Leaders*, EyeCareLeaders.com (last visited, Jun. 8, 2022), https://eyecareleaders.com/about-eye-care-leaders/
[2] *Id.*
[3] *Id.*

personal information documented by medical providers. Defendant serves thousands of clinics, which in turn serve hundreds of thousands of individuals every year, if not more. As such, Defendant's platforms contain a massive repository of Sensitive Information, acting as a particularly lucrative target for data thieves.[4]

17. Defendant understands the need to protect the Sensitive Information it possesses from wrongdoers. In one article, Eye Care Leaders states there are, "[f]ive key functions to look for in practice management software[.]"[5] This includes several recommendations that clinics choose a practice management software that adequately protects data and communications, noting that the platform should provide "secure communications" of information like "health care staff, notes about [patient] care, requests for prescription refills, details about past and upcoming visits, information about medication, and more." [6] Defendant also recommends that clinics choose software that provides a "secure online patient portal", "securely store[s] the insurance information of your patients" and "securely connect[s] patients with healthcare professionals for simple and secure communications."[7]

---

[4] *Id.*
[5] *Five key functions to look for in practice management software*, EyeCareLeaders.com (last visited, Jun. 8, 2022), https://eyecareleaders.com/key-functions-to-look-in-practice-management-software/
[6] *Id.*
[7] *Id.*

18. Eye Care Leaders also published an article providing a "One Step Guide for Independent Healthcare Practices to Improve Data Security."[8] There, Defendant acknowledged the risks of a data breach and the associated "staggering" costs:

> It feels like barely a month goes by without news of another high-profile healthcare data breach affecting thousands or even millions of people. These cyber attacks happen so often that we've probably become desensitized to the numbers. However, the cost of data breaches to healthcare practices is staggering. According to a recently published report, cyber attacks cost the healthcare industry $6.5 million annually. Not just this, more than 32 million patient records were breached in the first half of 2019 alone[.][9]

19. In hoping to convince clinics to purchase Eye Care Leaders' platforms to manage patients' Sensitive Information, Defendant warned clinics that "independent healthcare practices are more prone to cyber-attacks due to their weaker online security and fewer financial resources."[10] It further warned that "hackers know" the staff in independent clinics are "too busy to think about data security" and lack the "skills and budget to deploy the right technology and strong firewalls."[11] Thus, Eye Care Leaders claimed it was time for clinics to "sit up, smell the coffee" and take action, including, apparently, purchasing a "cloud-based EHR system[] capable of delivering enhanced

---

[8] *One Ste Guide for Independent Healthcare Practices to Improve Data Security*, EyeCareLeaders.com (last visited Jun. 8, 2022), https://eyecareleaders.com/one-step-guide-for-independent-healthcare-practices-to-improve-data-security/
[9] *Id.*
[10] *Id.*
[11] *Id.*

security than (sic) traditional paper records",[12] which Eye Care Leaders just so happened to have available for purchase.

20. Indeed, Eye Care Leaders promised clinics that its "office-based secure EHR systems" provided "software-as-a-service" that eliminated the need to "spend thousands of dollars buying and maintaining on-site servers . . . to host the system, including a server, hardware, and software, plus the systems [that] needed regular maintenance and management from one or more IT professional."[13] Rather, Eye Care Leaders provided "cost-effective" tools that "offer[ed] secure communication with patients and partners." All clinics needed to do was "log in and get to work."[14]

21. Apart from bragging about its software's cost-effectiveness and security, Eye Care Leaders also represented itself as a data security expert. It regularly issued articles providing advice to clinics on how to best manage data security and to protect patient records from being stolen by wrongdoers. In addition to its "One Step Guide for Independent Healthcare Practices to Improve Data Security", Eye Care Leaders wrote about "Six Tips to Improve Patient Data Security for Healthcare Practices," advising clinics, again, of the significant costs of a data breach and the substantial risks they pose to

[12] *Id.*
[13] *How cloud-based HER systems boost your cost-efficiency*, EyeCareLeaders.com (last visited Jun. 8, 2022), https://eyecareleaders.com/how-cloud-based-ehr-boosts-cost-efficiency/
[14] *Id.*

clinics and patients.[15] It advised clinics to: (1) perform a security risk assessment; (2) train employees on data security protocols; (3) establish security guidelines for external devices; (4) assign role-based access to data; (5) encrypt sensitive data; and (6) build a security-first culture.[16] Eye Care Leaders promised that "the above-mentioned best practices can ensure greater protection" and noted that clinics must "focus [their] efforts beyond compliance to ensure that patient data is safe and protected."[17]

22. Similarly, Eye Care Leaders wrote about ransomware, warning clinics that they "Should Worry About Ransomware" and providing advice on how to prevent a ransomware attack.[18] Eye Care Leaders claimed that "It's a People Problem" and that "[r]ansomware attacks often result from phishing scams[.]" In a subsequent article, Eye Care Leaders advised clinics of "4 Ways to Protect Your Practice from Ransomware Attacks", including to (1) get smart about ransomware, (2) don't skimp on training, (3) keep you protection current, and (4) build your team.[19]

23. Defendant was obligated to implement reasonably secure data measures because of its: (1) portrayal of itself as a data security expert with a secure software

---

[15] *Six Tips to Improve Patient Data Security for Healthcare Practices*, EyeCareLeaders.com (last visited Jun. 8, 2022), https://eyecareleaders.com/six-tips-to-improve-patient-data-security-for-healthcare-practices/
[16] *Id.*
[17] *Id.*
[18] *Why You Should Worry About Ransomware*, EyeCareLeaders.com (last visited Jun. 8, 2022), https://eyecareleaders.com/eye-care-cybersecurity-ransomware
[19] *4 Ways to Protect Your Practice from Ransomware Attacks*, EyeCareLeaders.com (last visited Jun. 8, 2022), https://eyecareleaders.com/protect-against-ransomware-attacks/

platform; (2) purported knowledge of the steps necessary to prevent a significant data breach; (3) acceptance of its clients' patients' highly sensitive records; and (4) knowledge of the possibility of a data breach should it fail to secure its platform.. Defendant acknowledged that its failure to reasonably safeguard its clients' Sensitive Information against a security breach could impose "staggering" costs on clinics and patients.

24. Defendant, however, did not reasonably protect, secure, or store Plaintiff's and the Class's Sensitive Information prior to, during, or after the Data Breach. Rather, it failed to employ reasonable data security measures. Defendant knew or should have known, its security was insufficient to reasonably protect the highly Sensitive Information it maintained.

25. Consequently, cybercriminals circumvented Defendant's security measures, resulting in a significant data breach that impacted hundreds of thousands, if not more.

B. Eye Care Leaders Suffered a Massive Data Breach, Exposing Patients' Sensitive Information

26. On or around December 4, 2021, a malicious actor gained unauthorized access to Defendant's myCare Identity solution, which included Defendant's databases, system configuration files, and data. By doing so, the actor gained access to the sensitive personal, medical, financial, and insurance information of Defendant's clients' current and former patients.

27. Upon information and belief, the actors viewed, copied and exfiltrated substantial amounts of Plaintiff's and the Class's PII and PHI. This included highly

sensitive information such as patient names, dates of birth, medical record numbers, health insurance information, Social Security numbers, and information regarding the care received at the affected eye care practices.

28. This is not Eye Care Leaders' first improper disclosure of patients' Sensitive Information. In March 2021, Eye Care Leaders suffered a ransomware attack that impacted its iMedicWare platform. That breach caused an outage of iMedicWare that lasted several days and disrupted clinic practices. Despite the fact the outage occurred due to a ransomware attack, Eye Care Leaders represented to its clients that the outage was due to a technical issue. It took Eye Care Leaders more than 30 days to restore the functionality of its iMedicWare platform.

29. On August 17, 2021, Eye Care Leaders purportedly suffered another attack related to its myCare Integrity platform. From August 20-27, 2021, Eye Care Leaders notified its clients at that time that myCare Integrity was suffering from "performance" or "system" issues when in reality, it was another ransomware attack. On August 28, 2021, Eye Care Leaders finally informed its clients of a ransomware attack caused by a former employee. Despite being terminated, the former employee retained his credentials to access patient information—a massive data security risk. With those credentials, the former employee accessed Eye Care Leaders's systems and orchestrated the attack.

30. Thus, the Data Breach here was Eye Care Leaders's *third data breach in less than ten months*.

31. As with its prior data breaches, Eye Care Leaders did not disclose the existence of the present Data Breach to its clients for weeks after learning of it, and still does not appear to have fully determined the scope of the breach or notified all impacted clinics.

32. Additionally, rather than notifying clients directly, Eye Care Leaders left it to its clients to issue notices to those impacted by the Data Breach. For example, on April 28, 2022, four months after the Data Breach, Summit Eye Associates notified its patients of the Data Breach.[20] Around the same time, EvergreenHealth issued notice to its impacted patients, noting that Eye Care Leaders had informed it of the Data Breach on March 1, 2022, and making clear that the "incident did not involve unauthorized access to any EvergreenHealth systems."[21]

33. The EvergreenHealth notice, which appears to have been drafted by Eye Care Leaders, included a recommendation that "patients whose information may have been involved in this incident review the statements they receive from their healthcare providers. If they see any services that were not received, they should contact the provider immediately."[22]

---

[20] *Eye Care Leaders Hack Impacts Hundreds of Thousands of Patients*, HIPPA Journal (May 12, 2022), https://www.hipaajournal.com/eye-care-leaders-hack-impacts-tens-of-thousands-of-patients/

[21] *Notice of Eye Care Leaders Data Security Incident*, EvergreenHealth.com (last visited, Jun. 8, 2022), https://www.evergreenhealth.com/about-us/notice-of-eye-care-leaders-data-security-incident/

[22] *Id.*

34. Since the initial notices of the Data Breach, other clinics have continued to provide notice to patients impacted by the Eye Care Leaders's Data Breach. For example, as recently as June 1, 2022, one clinic, Burman & Zuckerbrod Ophthalmology Associates, P.C. provided notice to 1,337 patients that their information may have been exposed by Eye Care Leaders. Additionally, on May 31, 2022, Associated Ophthalmologists of Kansas City, P.C. notified 13,461 patients that they may have been impacted by the Eye Care Leaders breach.

35. Numerous other eye care clinics have also recently reported data breaches to the U.S. Department of Health and Human Services but have not confirmed whether their events are related to Eye Care Leaders.

36. Currently, numerous clinics are known to have been impacted by the Data Breach, and likely many more are implicated. Those clinics known to have been impacted include:

a. Summit Eye Association

b. EvergreenHealth

c. Allie Eye Physicians & Surgeons

d. Regional Eye Associates, Inc. & Surgical Eye Center

e. Central Vermont Eye Care

f. Frank Eye Center

g. Arkfeld, Parson, and Goldstein, d/b/a Illumin

h. Northern Eye Care Associates

i. Ad Astra Eye

j. Burman & Zuckerbrod Ophthalmology Associates, P.C.

k. Sylvester Eye Care

l. Moyes Eye Center

m. Associated Ophthalmologists of Kansas City, P.C.

37. Notices issued to impacted patients regarding the Data Breach recommended Plaintiff and the Class take several time-consuming steps to mitigate the risk of future fraud and identity theft, such as creating fraud alerts, submitting documents to the IRS, and credit freezes.

38. Given that Defendant purposefully obtained and stored the PII and PHI of Plaintiff and the Class and knew or should have known of the serious risk and harm caused by a data breach, Defendant was obligated to implement reasonable measures to prevent and detect cyberattacks. This includes measures recommended by the Federal Trade Commission, required by the Health Insurance Portability and Accountability Act, and promoted by data security experts and other agencies. This obligation stems from the foreseeable risk of a Data Breach given that Defendant collected, stored, and had access to a swath of highly sensitive patient records and data and, additionally, because other highly publicized data breaches at different healthcare institutions put Defendant on notice that the higher personal data it stored might be targeted by cybercriminals.

39. Despite the highly sensitive nature of the information Defendant obtained, created, and stored, and the prevalence of health care data breaches, Defendant inexplicably

failed to take appropriate steps to safeguard the PII and PHI of Plaintiff and the Class. The Data Breach itself, and information Defendant has disclosed about the breach to date, including its length, the need to remediate Defendant's cybersecurity, the number of people impacted, and the sensitive nature of the impacted data, collectively demonstrate Defendant failed to implement reasonable measures to prevent the Data Breach.

C. Exposure of Sensitive Information Creates a Substantial Risk of Harm

40. The personal, health, and financial information of Plaintiff and the Class is valuable and has become a highly desirable commodity to data thieves.

41. Defendant's failure to reasonably safeguard Plaintiff's and the Class's sensitive PHI and PII has created a serious risk to Plaintiff and the Class, including both a short-term and long-term risk of identity theft and other fraud.

42. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

43. According to experts, one out of four data breach notification recipients becomes a victim of identity fraud.[23]

[23] *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims,* ThreatPost.com (last visited Jan. 17, 2022), https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/

44. Stolen Sensitive Information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines and is frequented by criminals, fraudsters, and other wrongdoers. Law enforcement has difficulty policing the "dark web," which allows users and criminals to conceal identities and online activity.

45. Moreover, according to Robert P. Chappell, Jr., a law enforcement professional, fraudsters can steal and use a minor's information until the minor turns eighteen years old before the minor even realizes he or she has been the victim of an identity theft crime.[24]

46. The risk to minor Class members is substantial given their age and lack of established credit. The information can be used to create a "clean slate identity," and use that identity for obtaining government benefits, fraudulent tax refunds, and other scams. There is evidence that children are 51% more likely to be victims of identity theft than adults.[25]

47. Purchasers of Sensitive Information use it to gain access to the victim's bank accounts, social media, credit cards, and tax details. This can result in the discovery and release of additional Sensitive Information from the victim, as well as Sensitive

[24] Brett Singer, *What is Child Identity Theft?*, Parents (last visited Jan. 17, 2022), https://www.parents.com/kids/safety/tips/what-is-child-dentity-theft/.
[25] Avery Wolfe, *How Data Breaches Affect Children*, Axion Cyber Sols. (Mar. 15, 2018) (last visited Jan. 18, 2022), https://axioncyber.com/data-breach/how-data-breaches-affect-children/.

Information from family, friends, and colleagues of the original victim. Victims of identity theft can also suffer emotional distress, blackmail, or other forms of harassment in person or online. Losses encompass financial data and tangible money, along with unreported emotional harms.

48. The FBI's Internet Crime Complaint (IC3) 2019 report estimated there was more than $3.5 billion in losses to individual and business victims due to identity fraud in that year alone. The same report identified "rapid reporting" as a tool to help stop fraudulent transactions and mitigate losses.

49. Defendant did not rapidly, or even reasonably timely, report to Plaintiff and the Class that their Sensitive Information had been exposed or stolen.

50. The Federal Trade Commission ("FTC") has recognized that consumer data is a lucrative (and valuable) form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour reiterated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[26]

51. The FTC has also issued, and regularly updates, guidelines for businesses to implement reasonable data security practices and incorporate security into all areas of the business. According to the FTC, reasonable data security protocols require:

---

[26] Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009) (last visited June 7, 2022) https://www.ftc.gov/news-events/news/speeches/remarks-ftc-exploring-privacy-roundtable

(1) encrypting information stored on computer networks;

(2) retaining payment card information only as long as necessary;

(3) properly disposing of personal information that is no longer needed or can be disposed of pursuant to relevant state and federal laws;

(4) limiting administrative access to business systems;

(5) using industry tested and accepted methods;

(6) monitoring activity on networks to uncover unapproved activity;

(7) verifying that privacy and security features function properly;

(8) testing for common vulnerabilities; and

(9) updating and patching third-party software.[27]

52. The United States Cybersecurity & Infrastructure Security Agency, and other federal agencies, recommend similar and supplemental measures to prevent and detect cyberattacks, including, but not limited to: implementing an awareness and training program, enabling strong spam filters, scanning incoming and outgoing emails, configuring firewalls, automating anti-virus and anti-malware programs, managing privileged accounts, configuring access controls, disabling remote desktop protocol, and updating and patching computers.

53. The FTC cautions businesses that failure to protect Sensitive Information and the resulting data breaches can destroy consumers' finances, credit history, and reputations, and can take time, money, and patience to resolve the fallout.[28] Indeed, the FTC treats the

[27] *Start With Security, A Guide for Business,* FTC (last visited June 7, 2022) https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

[28] Taking Charge, What to Do if Your Identity is Stolen, FTC (last visited June 7, 2022), https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0014-identity-theft.pdf

failure to implement reasonable and adequate data security measures—like Defendant failed to do here—as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

D. The Healthcare Industry is Particularly Susceptible to CyberAttacks.

54. A 2010 report focusing on healthcare data breaches found the "average total cost to resolve an identity theft related incident … came to about $20,000."[29] According to survey results and population extrapolations from the National Study on Medical Identity Theft report from the Ponemon Institute, nearly 50% of victims reported losing their healthcare coverage because of a data breach and nearly 30% reported an increase in their insurance premiums.[30] Several individuals were unable to fully resolve their identity theft crises. Healthcare data breaches are an epidemic and they are crippling the impacted individuals—millions of victims every year.[31]

55. According to an analysis of data breach incidents reported to the U.S. Department of Health and Human Services and the media, from 2015 and 2019 the number of healthcare related security incidents increased from 450 annual incidents to 572 annual incidents, likely a conservative estimate.[32]

---

[29] *See* Elinor Mills, *Study: Medical identity theft is costly for victims,* CNET (March 3, 2010), (last visited June 7, 2021), https://www.cnet.com/tech/services-and-software/study-medical-identity-theft-is-costly-for-victims/

[30] *Id.*

[31] *Id.*

[32] Heather Landi, *Number of patient records breached nearly triples in 2019*, FIERCE HEALTHCARE (Feb. 20, 2020), https://www.fiercehealthcare.com/tech/number-patient-records-breached-2019-almost-tripled-from-2018-as-healthcare-faces-new-threats#:~:text=OVer%2041%20million%20patient%20records,close%20to%2021%20million%20records (last visited Jan.19, 2022).

56. According to the Verizon Data Breach Investigations Report, the health care industry, including hospitals and other providers, experienced 655 known data breaches, 472 of which had confirmed data disclosures in 2021.[33] For the tenth year in a row, the healthcare industry has seen the highest impact from cyberattacks of any industry.[34]

57. As a vendor of healthcare clinics that provide services to hundreds of thousands of patients, if not more, Defendant knew or should have known the importance of protecting the Sensitive Information entrusted to it. Defendant also knew of the foreseeable and catastrophic consequences if its systems were breached. Despite this, Defendant failed to take reasonable data security measures to prevent or mitigate losses from cyberattacks.

E. Plaintiff and the Class's PHI and PII are Valuable.

58. Unlike financial information, such as credit card and bank account numbers, the PHI and certain PII exfiltrated in the Data Breach cannot be easily changed. Dates of birth and social security numbers are given at birth and attach to a person for the duration

[33] Verizon, 2021 Data Breach Investigations Report: Healthcare NAICS 62 (2021) (last visited Jan. 19, 2021), https://www.verizon.com/business/resources/reports/dbir/2021/data-breach-statistics-by-industry/healthcare-data-breaches-security/.

[34] *Five worthy reads: The never-ending love story between cyberattacks and healthcare,* ManageEngine, https://blogs.manageengine.com/corporate/manageengine/2021/08/06/the-never-ending-love-story-between-cyberattacks-and-healthcare.html#:~:text=According%20to%20Infosec%20Institute%2C%20credit,is%20%24158%20per%20stolen%20record.

of his or her life. Medical histories are inflexible. For these reasons, these types of information are the most lucrative and valuable to hackers.[35]

59. Birth dates, Social Security numbers, addresses, employment information, income, and similar types of information can be used to open several credit accounts on an ongoing basis rather than exploiting just one account until it's canceled.[36] For that reason, cybercriminals on the dark web are able to sell Social Security numbers for large profits. For example, an infant's social security number sells for as much as $300 per number.[37] Those numbers are often then used for fraudulent tax returns.[38]

60. Consumers place a considerable value on their Sensitive Information and the privacy of that information. One 2002 study determined that U.S. consumers highly value a website's protection against improper access to their Sensitive Information, between $11.33 and $16.58 per website. The study further concluded that to U.S. consumers, the collective "protection against error, improper access, and secondary use of personal

---

[35] *Calculating the Value of a Data Breach – What Are the Most Valuable Files to a Hacker?* Donnellon McCarthy Enters, https://www.dme.us.com/2020/07/21/calculating-the-value-of-a-data-breach-what-are-the-most-valuable-files-to-a-hacker/ (last visited June 7, 2022).

[36] *Anthem hack: Personal data stolen sells for 10x Price of Stolen Credit Card Numbers*, Tim Greene, https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited June 7, 2022).

[37] Selena Larson, *Infant Social Security Numbers are for sale on the dark* web, CNN Business, (last visited June 7, 2022), https://money.cnn.com/2018/01/22/technology/infant-data-dark-web-identity-theft/index.html.

[38] *Id.*

information is worth between $30.49 and $44.62.[39] This data is approximately twenty years old, and the dollar amounts would likely be exponentially higher today.

61. Defendant's Data Breach exposed a variety of Sensitive Information, including Social Security numbers and PHI.

62. The Social Security Administration ("SSA") warns that a stolen Social Security number can lead to identity theft and fraud: "Identity thieves can use your number and your credit to apply for more credit in your name."[40] If the identity thief applies for credit and does not pay the bill, it will damage victims' credit and cause a series of other related problems.

63. Social Security numbers are not easily replaced. In fact, to obtain a new number, a person must prove that he or she continues to be disadvantaged by the misuse—meaning an individual must prove actual damage has been done and will continue in the future.

64. PHI, also at issue here, is likely even more valuable than Social Security numbers and just as capable of being misused. The Federal Bureau of Investigation

[39] 11-Horn Hann, Kai-Lung Hui, *et al*, *The Value of Online Information Privacy: Evidence from the USA and Singapore,* at 17. Marshall Sch. Bus., Univ. So. Cal. (Oct. 2002), https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited June 7, 2022).

[40] Social Security Administration, *Identity Theft and Your Social Security Number*, (last visited June 7, 2022), https://www.ssa.gov/pubs/EN-05-10064.pdf.

("FBI") has found instances of PHI selling for fifty times the price of stolen Social Security numbers or credit card numbers.[41]

65. Other reports found that PHI is ten times more valuable on the black market than credit card information.[42] This is because one's personal health history, including prior illness, surgeries, diagnoses, mental health, and the like cannot be changed or replaced, unlike credit card information and even, under difficult circumstances, social security numbers. Credit card information and PII sell for on the black market, but PHI can sell for as much as $363 according to the Infosec Institute.[43]

66. Cybercriminals recognize and exploit the value of PHI and PII. The value of PHI and PII is the foundation to the cyberhacker business model.

67. Because the Sensitive Information exposed in Defendant's Data Breach is permanent data, there may be a gap of time between when it was stolen and when it will be used. The damage may continue for years. Plaintiff and the Class now face years of monitoring their financial and personal records with a high degree of scrutiny. The Class

---

[41] *FBI Cyber Division Bulletin: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI (April 8, 2014), https://publicintelligence.net/fbi-health-care-cyber-intrusions/ (last visited June 7, 2022).
[42] *Anthem hack: Personal data stolen sells for 10x Price of Stolen Credit Card Numbers*, Tim Greene, https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited June 7, 2022).
[43] *Hackers Selling Healthcare Data in the Black Market*, INFOSEC, https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited June 7, 2022).

has incurred and will incur this damage in additional to any fraudulent use of their Sensitive Information.

F. Defendant's Conduct Violates HIPAA

68. Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), individuals' health information must be:

> properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being. The Privacy Rule strikes a balance that permits important uses of information while protecting the privacy of people who seek care and healing.[44]

69. HIPAA is a "federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge."[45] The rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.[46]

70. HIPAA defines sensitive patient personal and health information as: (1) Name; (2) Home and work addresses; (3) Home and work phone numbers; (4) Personal

---

[44] U.S. Dept. of Health & Human Services: Summary of the HIPAA Privacy Rule (last visited June 7, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

[45] Health Insurance Portability and Accountability Act of 1996 (HIPAA), CDC, https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge. (last visited June 7, 2022).

[46] U.S. Dept. of Health & Human Services: Summary of the HIPAA Privacy Rule (last visited June 7, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

and professional email addresses; (5) Medical records; (6) Prescriptions; (7) Health insurance information; (8) Billing information; (9) Social Security number; (10) Spouse and children's information; and/or (11) Emergency contact information.[47]

71. To ensure protection of this private and sensitive information, HIPAA mandates standards for handling PHI—the very data Defendant failed to protect. The Data Breach resulted from Defendant's failure to comply with several of these standards:

a. Violation of 45 C.F.R. § 164.306(a)(1): failing to ensure the confidentiality and integrity of electronic protected health information that Defendant creates, receives, maintains, and transmits;

b. Violation of 45 C.F.R. § 164.312(a)(1): Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights;

c. Violation of 45 C.F.R. § 164.308(a)(1): Failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

d. Violation of 45 C.F.R. § 164.308(a)(6)(ii): Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity;

e. Violation of 45 C.F.R. §164.306(a)(2): Failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information;

f. Violation of 45 C.F.R. §164.306(a)(3): Failing to protect against any reasonably anticipated uses or disclosures of electronically protected health information that are not permitted under the privacy rules regarding individually identifiable health information;

[47] *Id.*

g. Violation of 45 C.F.R. §164.306(a)(94): Failing to ensure compliance with HIPAA security standard rules by its workforce;

h. Violation of 45 C.F.R. §164.502, et seq: Impermissibly and improperly using and disclosing protected health information that is, and remains, accessible to unauthorized persons; and

i. Violation of 45 C.F.R. §164.530(c): Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information.

72. Despite Defendant's failure to reasonably protect Plaintiff's and the Class's Sensitive Information, it has not offered any compensation or adequate remedy considering the significant and long-term risk Plaintiff and the Class face.

CLASS ALLEGATIONS

73. Plaintiff brings this class action pursuant to [Federal Rule of Civil Procedure 23 or State Law Provision] on behalf of themselves and all others similar situated, as representative of the following Class:

> All persons whose information was compromised by Eye Care Leaders's Data Breach or were sent notice that they were compromised by the Data Breach.

74. Excluded from the Class are Defendant; its officers, directors, and employees of Defendant; any entity in which Defendant has a controlling interest in, is a parent or subsidiary of, or which is otherwise controlled by Defendant; and Defendant's affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assignees. Also excluded are the Judges and Court personnel in this case and any members of their immediate families.

75. Plaintiff reserves the right to modify and/or amend the Class definition, including but not limited to creating additional subclasses, as necessary.

76. All members of the proposed Class are readily identifiable through Defendant's records.

77. **Numerosity.** The members of the Class are so numerous that joinder is impracticable. Plaintiff is informed and believes that the proposed Class includes hundreds of thousands of patients. The precise number of Class members is unknown to Plaintiff but may be ascertained from Defendant's records.

78. **Commonality and Predominance.** This action involves common questions of law and fact, which predominate over any questions only affecting individual Class members. These common legal and factual questions include, but are not limited to:

a. Whether Defendant owed Plaintiff and the other Class members a duty to adequately protect their Sensitive Information;

b. Whether Defendant owed Plaintiff and the other Class members a duty to implement reasonable data security measures due to the foreseeability of a data breach;

c. Whether Defendant owed Plaintiff and the other Class members a duty to implement reasonable data security measures because Defendant accepted, stored, created, and maintained highly sensitive information concerning Plaintiff and the Class;

d. Whether Defendant knew or should have known of the risk of a data breach;

e. Whether Defendant breached its duty to protect the PII and PHI of Plaintiff and Class members;

f. Whether Defendant knew or should have known about the inadequacies of its data protection, storage, and security;

g. Whether Defendant failed to use reasonable care and reasonable methods to safeguard and protect Plaintiff's and the Class's Sensitive Information from unauthorized theft, release, and disclosure;

h. Whether proper data security measures, policies, procedures and protocols were enacted within Defendant's offices and computer systems to safeguard and protect Plaintiff's and the Class's Sensitive Information from unauthorized theft, release or disclosure;

i. Whether Defendant's conduct was the proximate cause of Plaintiff's and the Class's injuries;

j. Whether Plaintiff and the Class suffered ascertainable and cognizable injuries as a result of Defendant's misconduct;

k. Whether Plaintiff and the Class are entitled to recover damages; and

l. Whether Plaintiff and the Class are entitled to other appropriate remedies including injunctive relief.

79. Defendant engaged in a common course of conduct giving rise to the claims asserted by Plaintiff on behalf of herself and the Class. Individual questions, if any, are slight by comparison in both quality and quantity to the common questions that control this action.

80. **Typicality.** Plaintiff's claims are typical of those of other Class members because Plaintiff's PHI and PII, like that of every other Class member, was misused and improperly disclosed by Defendant. Defendant's misconduct impacted all Class members in a similar manner.

81. **Adequacy.** Plaintiff intends to prosecute this case vigorously and will fairly and adequately represent and protect the interest of the members of the Class. Plaintiff has retained counsel experienced in complex consumer class action litigation. Plaintiff has no adverse or antagonistic interests to those of the Class.

82. **Superiority.** A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that would occur with individual litigation of their claims against Defendant. The adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudications of the asserted claims. There will be no difficulty in managing this action as a class action, and the disposition of the claims of the Class members in a single action will provide substantial benefits to all parties and to the Court.

CLAIMS

COUNT I
Negligence
(on behalf of Plaintiff and the Class)

83. Plaintiff realleges and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

84. Defendant collected, stored, and maintained Plaintiff's and the Class's Sensitive Information on behalf of clinics and provided medical and records retention software to clinics who served Plaintiff and the Class.

85. Plaintiff and the Class are a well-defined, foreseeable, and probable group of patients that Defendant was aware, or should have been aware, could be injured by inadequate data security measures. The nature of Defendant's business requires clinics to provide the Sensitive Information of its patients that Defendant unilaterally collects, maintains, and stores. That information includes medical histories, dates of birth, addresses, phone numbers, and medical insurance information. Therefore, as part of Defendant's services, it must use, handle, gather, and store the Sensitive Information of Plaintiff and the Class and, additionally, solicit and create records containing Plaintiff's and the Class's Sensitive Information.

86. A large depository of highly valuable health care information is a foreseeable target for cybercriminals looking to steal and profit from that sensitive information and Defendant warned clinics numerous times of the serious risk of a data breach and the need to implement reasonable data security.

87. Defendant knew or should have known that, given its repository of a host of Sensitive Information for hundreds of thousands of patients posed a significant risk of being targeted for a data breach. Thus, Defendant had a duty to reasonably safeguard its patients' data by implementing reasonable data security measures to protect against data breaches. The foreseeable harm to Plaintiff and the Class of inadequate data security created a duty to act to reasonably and safeguard the Sensitive Information.

88. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in safeguarding and protecting their Sensitive Information in its possession from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

89. This duty included, among other things, designing, maintaining, and testing its security systems to ensure that Plaintiff's and the Class's PHI and PII was adequately protected and secured. Defendant further had a duty to implement processes that would detect a breach of their security system in a timely manner.

90. Defendant also had a duty to timely disclose to Plaintiff and the Class that their Sensitive Information had been or was reasonably believed to have been compromised. Timely disclosure is necessary so that, among other things, Plaintiff and the Class may take appropriate measures to monitor their accounts for unauthorized access, to contact the credit bureaus to request freezes or place alerts and take all other appropriate precautions, including those recommended by Defendant.

91. Additionally, HIPAA creates industry standards for maintaining the privacy of health-related data. Defendant knew or should have known it had a legal obligation to

secure and protect Plaintiff's and the Class's Sensitive Information and that failing to do so is a serious violation of HIPAA.

92. Defendant also should have known that, given the Sensitive Information it held, Plaintiff and the Class would be harmed should it suffer a Data Breach. Defendant knew or should have known that their systems and technologies for processing and securing Plaintiff's and the Class's PHI and PII had security vulnerabilities susceptible to cyberattacks.

93. Despite that knowledge, Defendant failed to implement reasonable data security measures, which allowed cybercriminals to successfully breach Defendant's network and data environments, reside there undetected for a significant period of time, and access or steal a host of personal and healthcare information on thousands of Defendants' clients' patients.

94. Defendant failed to provide reasonable security for the data in its possession.

95. Defendant breached is duty to Plaintiff and the Class by failing to adopt, implement, and maintain reasonable security measures to safeguard their Sensitive Information, allowing unauthorized access to Plaintiff's and the Class's PHI and PII, and failing to recognize the Data Breach in a timely manner. Defendant further failed to comply with industry regulations and exercise reasonable care in safeguarding and protecting Plaintiff's and the Class's PHI and PII.

96. But for Defendant's wrongful and negligent breach of its duties, Plaintiffs' Sensitive Information would not have been accessed and exfiltrated by unauthorized

persons, and they would not face a risk of harm of identity theft, fraud, or other similar harms.

97. As a result of Defendant's negligence, Plaintiff and the Class suffered damages including, but not limited to, ongoing and imminent threat of identity theft crimes; out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or fraud; credit, debit, and financial monitoring to prevent and/or mitigate theft, identity theft, and/or fraud incurred or likely to occur as a result of Defendant's security failures; the value of their time and resources spent mitigating the identity theft and/or fraud; decreased credit scores and ratings; and irrecoverable financial losses due to fraud.

98. Consequently, Plaintiff seeks actual and compensatory damages, injunctive relief, attorneys' fees and expenses, and all other remedies available under law.

COUNT II
Negligence *Per Se*
(on behalf of Plaintiff and the Class)

99. Plaintiff reallege and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

100. Eye Care Leaders's conduct constitutes negligence *per se* because it was in violation of several statues enacted for the safety and protection of the public, including Plaintiffs and the Class.

101. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair ... practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade

Commission ("FTC"), the unfair act or practice of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

102. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and the Class's PHI and PII and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, the foreseeable consequences of a data breach, and Defendant's knowledge that inadequate data security could result in a data breach that imposes "staggering" costs on clinics and patients.

103. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

104. The harm that has occurred and been imposed on Plaintiff and the Class is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and the proposed Class.

105. Additionally, Defendant's violation of HIPAA constitutes negligence *per se*.

106. HIPAA, 45 C.F.R. Part 164 governs "Security and Privacy," with Subpart A providing "General Provisions," Subpart B regulating "Security Standards for the Protection of Electronic Protected Health Information," Subpart C providing requirements for "Notification in the Case of Breach of Unsecured Protected Health Information." Under 45 C.F.R. § 164.306, HIPAA "standards, requirements and implementation

specifications" apply to covered entities, such as Defendant. HIPAA requires Defendant to "ensure the confidentiality, integrity, and availability of all electronic protected health information" it receives and to protect against any "reasonably anticipated threats or hazards to the security or integrity" of the Sensitive Information. 45 C.F.R. § 164.306.

107. Defendant also violated HIPAA by failing to adhere to and meet the requirements of 45 C.F.R. §§ 164.308, 164.310, 164.312, 164.314, and 164.316.

108. Defendant also violated HIPAA by failing to use reasonable measures to protect the PII and PHI of Plaintiff and Class. Defendant's conduct was especially unreasonable given the nature of the Sensitive Information and the number of patients it serves, some of which are minors or patients who live below the federal poverty level, who may not have the means to expend significant amounts of time and money to fully mitigate the fallout of the Data Breach.

109. Finally, Defendant's violation of N.C. Gen. Code Stat. § 75-65 constitutes negligence *per se.* This statute requires businesses operating in North Carolina to provide "notice to the affected person that there has been a security breach following discovery or notification of the breach." Notice must be made "without unreasonable delay."

110. Both HIPAA and N.C. Gen. Stat. § 75-65 require timely notice of data breaches to each impacted consumer. HIPAA requires notice to be issued "in no case later than 60 calendar days after discovery of the breach." 45 C.F.R. § 164.404. North Carolina requires notice to be issued "without unreasonable delay." N.C. Gen. Stat. § 75-65(a). Both provisions require notice to include certain minimum information, including, but not

limited to a description of what the entity is doing to investigate the breach and mitigate harm.

111. Defendant breached HIPAA's and North Carolina's notification requirements by failing to give timely and complete notice. Defendant waited approximately three months from the date it was made aware of the Data Breach to notify the clinics, who are still issuing notices to the victims.

112. As a direct and proximate result of Defendant's violations of the FTC Act, HIPPA, and North Carolina's data breach statute, Plaintiff and the Class have been injured and are entitled to damages in an amount to be proven at trial.

113. Plaintiff seeks actual and compensatory damages, injunctive relief, attorneys' fees and expenses, and all other remedies available under the law.

COUNT III
Violation of North Carolina's Unfair and Deceptive Trade Practices Act
(on behalf of Plaintiff and the Class)

114. The North Carolina Unfair and Deceptive Trade Practices Act ("NCUDTPA") prohibits "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce[.]" N.C. Gen. Stat. § 75-1.1(a).

115. Under the act, "commerce" includes "all business activities, however, denominated[.]" *Id.* at § 75-1.1(b).

116. Furthermore, "any person . . . injured . . . by reason of any act or thing done by any other person, firm or corporation in violation of this Chapter, such person . . . so injured shall have a right of action on account of such injury done[.]" *Id.* at § 75-16.

117. Eye Care Leaders's conduct was unfair and deceptive in violation of the NCUDTPA. Specifically, Eye Care Leaders represented that it could adequately protect health care clinics' patient information and that its platforms were safe and secure. It solicited business through these representations and, in turn, gained access to and control over Plaintiff's and the Class's data, even without their knowledge.

118. Eye Care Leaders, however, could not adequately protect patient data, and designed an insecure platform lacking reasonable data security measures that were entirely inadequate to protect the highly sensitive data it collected and stored. Eye Care Leaders, furthermore, knew of defects in its systems and platforms and, in 2021 alone, suffered from three different data breaches. Moreover, despite advising clinics of the importance of data security measures, Eye Care Leaders failed to implement even basic measures. Its own former employee leveraged unrestricted access to Defendant's systems and servers to access patient data. Basic, long established data security standards require companies to restrict such access after terminating an employee. Eye Care Leaders failed to follow that baseline protocol.

119. Defendant's conduct after each of its data breaches, including the Data Breach at issue here, exacerbated the harm caused by its unreasonable data security

measures by representing that the data breaches were merely technical or systems issues, rather than admitting to their severity.

120. Under N.C. Gen. Stat. §§ 75-61, 75-65, businesses impacted by a data breach must provide notice without reasonable delay. Eye Care Leaders, however, waited almost three months to notify the clinics of the scope and extent of the Data Breach. Because Eye Care Leaders required the clinics to notify the impacted patients rather than notifying them on its own, Eye Care Leaders caused further delays to in the notice to customers.

121. Defendant's conduct was, thus, unethical, unscrupulous, substantially injurious to patients, and against North Carolina's stated policy of quickly providing notice of a data breach.

122. Defendant's conduct was also in and affecting commerce because it concerned the provision of services at healthcare clinics. Specifically, Eye Care Leaders provided software to its customers, the healthcare clinics, which in turn facilitated the provision of healthcare related services, including ophthalmology and optometry services, to patients.

123. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class members suffered and continue to suffer injuries and are entitled to damages in an amount to be proven at trial.

124. Plaintiff seeks actual and compensatory damages, injunctive relief, attorneys' fees and expenses, and all other remedies available under the law.

COUNT IV
Declaratory Judgment
(on behalf of Plaintiff and the Class)

125. Plaintiff realleges and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

126. Pursuant to 28 U.S.C. § 2201(a), this Court has the power to declare rights, status, and other legal relations, whether or not further relief is or could be claimed. Further, this Court has the power to declare either affirmative or negative decrees in form and effect, such as restraining acts that violate the laws described in this Complaint.

127. Whether Defendant's actions caused the Data Breach and subsequent harm to Plaintiff and the Class, and whether Defendant is presently maintaining adequate data security measure to safeguard Plaintiff's and the Class from further data breaches is an actual controversy.

128. Plaintiff and the Class are at a substantial and imminent risk of further compromise of their Sensitive Information. This is true irrespective of whether Plaintiff and the Class are current patients of Defendant because Defendant still maintains a swath of Plaintiff's and the Class's Sensitive Information. It suffered three data breaches within less than 10 months in 2021, and whether Eye Care Leaders has the ability and technical skill to prevent additional data breaches is not clear.

129. Therefore, this Court should enter a judgment declaring the following:

a. Defendant owed a legal duty, at the time of the Data Breach, to Plaintiff and members of the proposed Class to reasonably protect and

secure their Sensitive Information under the common law, HIPAA, FTC Act, 15 U.S.C. § 45(a)(1), and FCRA, 15 U.S.C. § 1681(b);

b. Defendant owed a legal duty to Plaintiff and members of the proposed Class to provide timely notice of the Data Breach under the common law, HIPAA, FTC Act, 15 U.S.C. § 45(a)(1), and FCRA, 15 U.S.C. § 1681(b);

c. Defendant continues to owe a legal duty to Plaintiff and members of the proposed Class to protect and secure their Sensitive Information under the common law, HIPAA, FTC Act, 15 U.S.C. § 45(a)(1), and FCRA, 15 U.S.C. § 1681(b); and

d. Defendant continues to owe a legal duty to Plaintiff and members of the proposed Class to provide timely notice of data breaches under the common law, HIPAA, FTC Act, 15 U.S.C. § 45(a)(1), and FCRA, 15 U.S.C. § 1681(b).

PRAYER FOR RELIEF

130. WHEREFORE, Plaintiff respectfully prays for judgment and relief as follows:

a. Certification the Class pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure and an order that notice be provided to all Class Members;

b. Designation of Plaintiff as Class representative and the undersigned counsel, Zimmerman Reed LLP, as Class Counsel;

c. An award of damages in an amount to be determined at trial or by this Court;

d. An order for injunctive relief, enjoining Defendant from engaging in the wrongful and unlawful acts described herein;

e. An award of statutory interest and penalties;

f. An award of costs and attorneys' fees; and

g. Such other relief the Court may deem just and proper.

DEMAND FOR TRIAL BY JURY

131. Plaintiff hereby demands a trial by jury of all issues so triable.

Respectfully submitted,

Dated: July 8, 2022

/s/T. Ryan Langley

T. Ryan Langley
NC Bar # 51273
Hodge & Langley Law Firm
229 Magnolia St.
Spartanburg, SC 29306
864-585-3873 – phone
864-585-6485 – fax
rlangley@hodgelawfirm.com

Brian C. Gudmundson (*Pro hac vice* forthcoming)
Jason P. Johnston (*Pro hac vice* forthcoming)
Michael J. Laird (*Pro hac vice* forthcoming)
Rachel K. Tack (*Pro hac vice* forthcoming)
ZIMMERMAN REED LLP
1100 IDS Center

80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
Facsimile: (612) 341-0844
brian.gudmundson@zimmreed.com
jason.johnston@zimmreed.com
michael.laird@zimmreed.com
rachel.tack@zimmreed.com